UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/578,633	05/25/2000	Steven Branigan	1-1-7	5753

22046 7590 06/29/2006

LUCENT TECHNOLOGIES INC.
DOCKET ADMINISTRATOR
101 CRAWFORDS CORNER ROAD - ROOM 3J-219
HOLMDEL, NJ 07733

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/578,633	BRANIGAN ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-12,14-24,26 and 27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-12,14-24,26 and 27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on March 26, 2006. Original application contained Claims 1-27. Applicant previously amended Claims 1-2, 6-11, 14,15, 6, 18-24, and 26-27. Applicant previously cancelled 4-5, 13, and 25. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn. Therefore, presently pending claims are 1-3, 6-12, 14-24, and 26-27.

Response to Arguments

Applicant's arguments with respect to claim 12, 14-24, and 26-27 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. Claim 1,10, 16, 21, and 24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains,

or with which it is most nearly connected, to make and/or use the invention. The subject matters "security characteristic" and "an indication of connectivity" is not enabled in the specification, and it is not clear what is being measured regarding security characteristic of the probed network when measuring characteristic is only an indication of connectivity. Is measure of indication of connectivity pertains to available bandwidth, traffic load or the integrity of the network? .

2. Claim 7, 20, and 23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The limitation "different security levels" is not defined and described in the specification. Does "different security levels" means access authentication for users, or security policy implemented on the network in general and on firewall in particular?

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1-3, 6-12, 14-24, and 26-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Schuba et al (USP 6,725,378).

As per claims 1 and 24, Schuba et al teach a communications network security method for ascertaining the integrity of a first communication network and identifying potential security risks across a perimeter of the first communications network, the method comprising: identifying a plurality of routes that define the first communications network, identifying a plurality of hosts as a function of the plurality of routes, performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network; probing at least one first host of the plurality hosts by transmitting a packet to the first host, the first host being selected from the census results and the packet having at least a source address of a second host which is associated with a second communications network determined as a function of the topology, wherein the source address is selected independent of any request from the second host to the first host (Fig.3-4, 7 and col. 6 line 46 to col.7 line 10, and col.7 line 50 to line 62), and

determining a security characteristic of the probed first host as a function of a response by the probed first host in receiving the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network the measure of connectivity being an indication of connectivity between first communication network and the second communication network (col. 12line 15 to line 32).

As per claim 10, Schuba et al teach a method for analyzing network security across a perimeter of a first communications network utilizing a security host, the method comprising:

receiving a census of the first communication network; transmitting, from the security host a packet associated with a host of a second communications network to a particular one host of the plurality of hosts internal to the communications network, the internal host being selected from the census, and the packet having an IP source address associated with the host of the second communications network, wherein the IP source address is selected independent of any request from the host of the second communications network to the internal host of the first communications network (Fig.3-4, 7 and col. 6 line 46 to col.7 line 10, and col.7 line 50 to line 62); and

determining a security characteristic of the particular one internal host as a function of a response by the internal host to the receipt of the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network (col. 12line 15 to line 32).

As per clam 16, Schuba et al teach a communications system for ascertaining the integrity of a first communication network and identifying potential security risks across a perimeter of the first communication network, the communication system comprising:

a first plurality of computers associated with the first communications network; a second plurality of computers associated with a second communications network, and a security host computer which determines a security characteristic of a first computer from the first plurality of computers, the security characteristic being a measure of connectivity between the first

communications network and the second communications network, performs a census of the communications network as a function of the first plurality of computers, and probes the first computer by transmitting a packet to the first computer, the first computer being selected from the census results and the packet being generated as a function of an IP source address associated with a second computer of the second plurality of computers, wherein said IP source address is selected independent of any request from the second computer to the first computer, and an IP address associated with the first computer (Fig.3-4, 7 and col. 6 line 46 to col.7 line 10, and col.7 line 50 to line 62), and

determining a security level associated with the first computer as a function of a response of the first computer to receiving the packet the measure of connectivity being an indication of connectivity between the first communications network and the second communication network (col. 12line 15 to line 32).

As per claim 21, Schuba et al teach a security host computer for ascertaining the integrity of a first communication network and identifying potential security risks across a perimeter of the first communication network, the security host computer comprising:

means for performing a census of the communications network and determining a topology of a first communications network, the topology being defined by at least one computer, means for probing the at least one computer by transmitting a packet to the computer, the computer being selected from the census results and the packet being generated as a function of (i) the topology, (ii) an IP source address associated with a particular host computer associated with a second communications network, wherein the IP source address is selected independent of

any request from the second computer to the first computer and (iii) an IP address associated with the computer, the second communications network being separate from the first communications network (Fig.3-4, 7 and col. 6 line 46 to col.7 line 10, and col.7 line 50 to line 62); and

a monitor for determining a security level of the computer as a function of a response by the computer to the receipt of the packet the security characteristic being a measure of connectivity between the first communications network and the second communications network (col. 12 line 15 to line 32).

As per claims 2, Schuba et al teach the source address of the second is a return IP address (col. 8 line 3 to line 17).

As per claims 3 and 26, Schuba et al teach the response of the probed first host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (col.8 line 18 to line 34).

As per claim 6, Schuba et al teach the determining the security characteristic operation further comprises: monitoring the probed first host to determine the response, and if the response includes a transmission of a second packet from the probed first host to the second host at the return IP address, generating a security alert message identifying the probed first host as a security risk (col.8 line 35 to col.9 line 3).

As per claim 7, Schuba et al teach the first and second communications network have different security levels (col. 9 line 4 to line 15).

As per claim 8, Schuba et al teach the transmitted packet is a TCP packet (col. 4 line 21 to line 52).

As per claim 9, Schuba et al teach the second packet is a UDP packet or an ICMP packet (Fiug.3, col.3 line 16 to line 45)).

As per claim 11, Schuba et al teach the determining the security characteristic operation further comprises: monitoring the probed host to determine the response, and if the response includes a transmission of a second packet, utilizing the IP source address, from the internal host to the host of the second communication network, generating a security alert message identifying the probed host as a security risk (col.8 line 35 to col.9 line 3, and col.10 line 32 to line 67).

As per claim 12, Schuba et al teach the second packet is derived using at least a portion of information from the transmitted packet (col.8 line 18 to line 34).

As per claim 14, Schuba et al teach the internal host is a dual-homed host (Fig.3).

As per claim 15, Schuba et al teach the security characteristic includes an indication that the probed host is outside any security measures provide by a firewall associated with the communications network (Fig.3, and col.6 line 46 to line 62).

As per claim 17, Schuba et al teach the security host computer is associated with the first communications network (Fig.3).

As per claim 18, Schuba et al teach the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (col.8 line 8 to line 34).

As per claim 19, Schuba et al teach the determining the security characteristic operation further comprises: monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (col.8 line 35 to col.9 line 3, and col.10 line 32 to line 67).

As per claims 20 and 27, Schuba et al teach the first communications network is an intranet and the second communications network is an Internet and the two network communications have different security levels (col. 6 line 54 to col. 7 line 10)

As per claim 22, Schuba et al teach the measure of connectivity is determined by monitoring the computer the response, and if the response includes a transmission of a second packet, utilizing the IP source address, from the computer, a security alert message identifying the computer as a security risk is generated (col.8 line 35 to col.9 line 3).

As per claim 23, Schuba et al teach the security level is determined with respect to a firewall located between the first communications network and the second communications network (Fig.3, and col.6 line 46 to line 62).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
June 10, 2006